# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/833,005 | 04/12/2001 | Douglas A. Hardy | GE04591 | 9509 |

7590 10/04/2007

Stanley A. Schlitter
JENNER & BLOCK, LLC
One IBM Plaza
Chicago, IL 60611

| EXAMINER | |
|---|---|
| SHIFERAW, ELENI A | |
| ART UNIT | PAPER NUMBER |
| 2136 | |
| MAIL DATE | DELIVERY MODE |
| 10/04/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

mn

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>09/833,005 | **Applicant(s)**<br>HARDY ET AL. | |
| | **Examiner**<br>David G. Cervetti | **Art Unit**<br>2136 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *16 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-20,23-25 and 28-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20,23-25 and 28-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Applicant's arguments filed July 16, 2007, have been fully considered but are not persuasive.

2. Claims 1-20, 23-25, and 28-30 are pending and have been examined. Claims 21, 22, 26, and 27 have been cancelled.

### *Response to Amendment*

3. The following prior art has been used in this action: Merrick USPN 5,416,841, hereinafter Merrick, Nakamura et al. USPN 6,457,126 B1, hereinafter Nakamura, Rasmussen et al. USPN 5,301,247, hereinafter Rasmussen, Kitajima et al. USPN 6,823,069 B1, hereinafter Kitajima, Vincent US Pub. No.: US 2004/0015953 A1, hereinafter Vincent, Mizikovsky USPN 6,853,729 B1, hereinafter Mizikovsky, Chan USPN 5,150,407, hereinafter Chan.

4. Regarding Applicant's argument that Merrick does not teach key splitting, Examiner respectfully submits that Merrick does in fact teach such feature (col.3, lines 35-65), where the full key is formed by two components and a splitting the key into two components, thus providing the teachings for the feature found in claims 1 and 11. **Applicant's arguments are not persuasive.**

### *Claim Rejections - 35 USC § 103*

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. **Claims 1-4 and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merrick, and further in view of Nakamura.**

**Regarding claim 1**, Merrick discloses

- a method for enabling encryption and decryption of an initial version of a software product (col. 2 lines 26-54) comprising the steps of:
- generating a first encryption key (fig. 1 element 40;full key~full-length key of N/N bits); encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product (col. 2 lines 26-27 and claim 1; encrypting data using key of length N); splitting said first encryption key into first and second key portions (col. 2 lines 47) by (i) generating a first key portion of said first encryption key (fig. 1 element 30 and col. 5 lines 6; short key/first key/n bits); and (ii) calculating a second key portion by utilizing said first key portion and said first encryption key to generate said second key portion of said first encryption key such that the combination of said first key portion and second'key portion form said first encryption key (col. 5 lines 6-11); providing said first key portion and said second key portion and said encrypted initial software product for use in a hardware product (col. 5 lines 33-52); combining said first key portion and said second key portion to provide said first encryption key in said hardware product (col. 5 lines 33-52); and utilizing said first encryption key to decrypt said encrypted initial software product in said hardware product (col. 5 lines 33-52 and claims 1, 6-7).

Merrick fails to disclose the first key portion is independent of information identifying said hardware product.

However it is very well known to generate a key from identifying information independent from hardware product.

Nakamura discloses generating encryption key 3, and key 1 from password which is independent of identifying information from hardware product (col. 18 lines 50-61, col. 19 lines 37-59, fig. 12 & 13, claim 11, col. 6 lines 38-39, and col. 3 lines 20-22) and also generating encrypting key based on random number information and encryption key 2 is disclosed on (col. 2 lines 52-59 and col. 14 lines 13-19).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Nakamura within the system of Merrick because they are analogous in data encryption.

One would have been motivated to incorporate the teachings of Merrick because it is known at the time of the invention and would generate the key based on key information, and/or password information so the generated key would identify the key or password of the user rather than the hardware name/serial number.

**Regarding claim 2**, the references disclose the method wherein said step of generating a first encryption key utilizes a ransom number generator to generate said first encryption key (Merrick col. 5 lines 5-16, Nakamura col. 13 lines 51-57).

**Regarding claim 3**, Merrick discloses the method wherein said step of calculating a second key portion utilizing an "exclusive or" logic operation to combine said first key portion and said first encryption key to calculate said second key portion (claim 7; a combiner combining first' and second key portions to generate a full length key). It is obvious that the combiner used in Merrick is an "exclusive or" logic. But the examiner provides reference Rasmussen that discloses xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK) using an exclusive or operator see, fig. 4 element 144 and col. 8 lines 40-48.Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of exclusive or within the combination system to combine the first encryption key and first key portion because operator exclusive or necessary for combining. One would have been motivated to do so to combine the first split portion of the key with the encryption key/decryption key.

**Regarding claim 4**, Merrick discloses wherein said step of combining said first key portion and said second key portion utilizes an "exclusive or" logic operation to combine said first key portion and said second key portion to provide said first encryption key (claim 7; a combiner combining first and second key portions to generate a full length key). It is obvious that the combiner used in Merrick is an "exclusive or" logic. But the examiner provides reference Rasmussen that discloses xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK) using an exclusive or operator see, fig. 4 element 144 and col. 8 lines 40-48.Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of excusive or within the combination system to combine the first encryption key and first key portion because operator exclusive or necessary for combining. One would have been motivated to do so to combine the first split portion of the key with the encryption key/decryption key.

**Regarding claim 23**, Nakamura discloses the method wherein said first key portion is generated independent of information generated in or by said hardware product (Nakamura, col. 18 lines 50-61, col. 19 lines 37-59, fig. 12 & 13, claim 11, col. 6 lines 38-39, and col. 3 lines 20-22). The rational for combining are the same as claim 1 above.

**Regarding claim 24**, Nakamura discloses the method wherein said second key portion is generated independent of said hardware product and any information specific to, identifying, or generated in or by said hardware product (Nakamura, col. 18 lines 50-61, col. 19 lines 37-59, fig. 12 & 13, claim 11, col. 6 lines 38-39, and col. 3 lines 20-22). The rational for combining are the same as claim 1 above.

**Regarding claim 25**, Nakamura discloses wherein said first encryption key is generated independent of said hardware product and any information specific to, identifying, or generated in or by said hardware product (Nakamura, col. 2 lines 52-59 and col. 14 lines 13- 19). The rational for combining are the same as claim 1 above.

7. **Claims 5-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merrick in view of Nakamura and further in view of Kitajima.**

**Regarding claim 5**, Merrick and Nakamura teach the method further enabling of said first encryption key to provide a second encryption key to secure a different version of the initial software product, further comprising the steps of: generating the second encryption key (Merrick fig. 1 element 40;full key~full-length key of N/N bits); encrypting the different version of the initial software product with the second encryption key to provide an encrypted different version of the software product (Merrick col. 2 lines 26-27 and claim 1 ; encrypting data using key of length N); combining the first encryption key and the second encryption key to provide a third key portion (Merrick col. 5 lines 33-52); installing said third key portion and the encrypted different version of the software product in said hardware product (Merrick col. 5 lines 5-52); combining said third key portion and said second key portion to generate a fourth key portion in said hardware product (Merrick col. 5 lines 33-52); combining the first key portion and the fourth key portion to provide said second encryption key in said hardware product (Merrick col. 5 lines 33-52); and using the second encryption key to decrypt the encrypted different version of the software product (Merrick col. 5 lines 33-52 and claims 1, 6-7). Merrick and Nakamura fail to teach an update of the keys.

However Kitajima discloses dividing encrypting key into a first half portion and a second half portion and periodically updating/changing keys and encryption algorithm to securely protect cryptograms against urmuthorized people (col. 11 lines 1-10). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of updating keys within the combination system because it would allow a secure data/message/information transmission (col. 11 lines 1-10). One would have been motivated to update the encryption key and the key portions to enhance security by making the keys unpredictable.

**Regarding claim 6**, references disclose the method wherein said step of generating a second encryption key utilizes a ransom number generator to generate said first encryption key (Merrick col. 5 lines 5-16, Nakamura col. 13 lines 51-57).

**Regarding claim 7**, Merrick discloses the method wherein said step of combining the first encryption key and the second encryption key utilizes an "exclusive or" logic operation to combine said first encryption key and said second encryption key to generate said third key portion (claim 7; a combiner combining first and second key portions to generate a full length key). It is obvious that the combiner used in Merrick is an "exclusive or" logic. But the examiner provides reference Rasmussen that discloses xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK) using an exclusive or operator see, fig. 4 element 144 and col. 8 lines 40-48. Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of excusive or within the combination system to combine said first encryption key and said second encryption key and generate said third key portion because operator exclusive or necessary for combining. One would have been motivated to do so to combine first encryption key and said second encryption key.

**Regarding claim 8**, Merrick teaches wherein said step of providing said second encryption key utilizes an "exclusive or" logic operation to combine said first key portion and said fourth key portion to provide said second encryption key (claim 7; a combiner combining first and second key portions to generate a full length key). It is obvious that the combiner used in Merrick is an "exclusive or" logic. But the examiner provides reference Rasmussen that discloses xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK) using an exclusive or operator see, fig. 4 element 144 and col. 8 lines 40-48. The rational for combining are the same as claim 7 above.

**8. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Merrick in view of Nakamura and further in view of Kitajima and further in view of Vincent.**

**Regarding claim 9**, the combination discloses all the subject matter as described above. The combination fail to disclose wherein said initial version of software product and said different version of said initial version of said software product are non-sequential versions. However Vincent discloses updating required versions out of multiple different versions of software products in non-sequential order (fig. 9 and par. 0071; updating component B from version 4 to version 6 and updating full component of D and E to version 1 and 2 respectively). Therefore it would have been obvious to one having ordinary skill in the art at the time. of the invention was made to employ the teachings of Vincent within the combination system because it would save time (par. 0015). One would have been motivated to update non-sequential version of software because it would allow a minimal time to download specific software components in contrast to conventional methods of updating software (par. 0015).

**9. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Merrick in view of Nakamura and further in view of Kitajima and further in view of Mizikovsky.**

**Regarding claim 10**, the combination discloses all the subject matter as described. The combination fail to teach wherein the second encryption key is non-sequential with said first encryption key. However Mizikovsky teaches an update key which is non-sequential with said first encryption key (col. 8 lines 21-43 and fig. 4; update key being different from new key.., generated in using RAND numbers). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Mizikovsky within the combination system because it would enhance security. One would have been motivated to incorporate the teachings of updating keys in non-sequential order to prevent unauthorized device from learning encryption keys and perform unauthorized decryption of content.

**10. Claims 11-14 and 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merrick in view of Nakamura and Chan.**

**Regarding claim 11**, Nakamura discloses a method for providing for the security of encryption keys for encryption and decryption of an initial version of a software product provided by a provider to a user of a hardware product (col. 2 lines 26-54), said method comprising: providing a first encryption key (fig. 1 element 40;fuli key~full-length key of N/N bits); encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product (col. 2 lines 26-27 and claim 1; encrypting data using key of length N); splitting said first encryption key into first and second key portions (col. 2 lines 47) by (i) generating a first key portion of said first encryption key(fig. 1 element 30 and col. 5 lines 6; short key/first key/n bits); and (ii) utilizing said first key portion and said first encryption key to calculate a second key portion of said first encryption key such that the combination of said first and second key portions form said first encryption key (col. 5 lines 6-11); storing said encrypted software product in a further memory means in the hardware product (col. 5 lines 33); combining said first key portion and said second key portion in the hardware product to provide said first encryption key (col. 5 lines 33-52); and decrypting said encrypted initial software product with said first encryption key (col. 5 lines 33-52 and claims 1, 6-7). Merrick fails to disclose the first key portion is independent of information identifying said hardware product. However it is very well known to generate a key from identifying information independent from hardware product. Nakamura et al. discloses generating encryption key 3, and key 1 from password which is independent of identifying information from hardware product (see col. 18 lines 50-61, col. 19 lines 37-59, fig. 12 & 13, claim 11, col. 6 lines 38-39, and col. 3 lines 20-22) and also generating encrypting key based on random number information and encryption key 2 is disclosed on (col. 2 lines 52-59 and col. 14 lines 13-19). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Nakamura et al. within the system of Merrick because they are analogous in data encryption. One would have been motivated to incorporate the teachings of Merrick because it is known at the time of the invention and would generate the key based on key information, and/or password information so the generated key would identify the key or password of the user rather than the hardware name/serial number. The combination teach storing key N-n in storage unit 26 of the key management system and storing the n bit first key separate from the second key in the user device because it would allow anyone obtaining access to the key management system to potentially decode the encrypted data ifn bit first key or any information about first key is stored in the key management system (see Merrick col. 5 lines 17-28) but does not explicitly disclose storing said first key portion in storage means external to the hardware and storing said second key portion separately from said first key portion in a tamper proof memory means in the hardware product. However Chan teaches encrypting digital data using encryption key, dividing encryption key in to two portions (col. 5 lines 44-45) and storing the portions of the key in two different storage devices (col. 5 lines 45-47, and col. 9 lines 6-14), and combining the portions of the keys in order to decrypt the encrypted digital data (col. 9 lines 28-30). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Chan within the combination system because they are analogous in key generation and data encryption. One would have been motivated to do so for secure use of decryption keys and data protection and/or the user cannot access the other portion easily.

**Regarding claim 12**, the references disclose the method wherein said step of generating a first encryption key utilizes a ransom number generator to generate said first encryption key (Merrick col. 5 lines 5-16, Nakamura col. 13 lines 51-57, Chan col. 5 lines 39-64).

**Regarding claim 13**, Merrick discloses the method wherein said step of calculating a second key portion utilizing an "exclusive or" logic'operation to combine said first key portion and said first encryption key to calculate said second key portion (claim 7; a combiner combining first and second key portions to generate a full length key). It is obvious that the combiner used in Merrick is an "exclusive or" logic. But the examiner provides reference Rasmussen that discloses xoring first portion of key (DEK 1) with second portion (DEK2) of key to form encryption key (DEK) using an exclusive or operator see, fig. 4 element 144 and col. 8 lines 40-48.Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of excusive or within the combination system to combine the first encryption key and first key portion because operator exclusive or necessary for combining. One would have been motivated to do so to combine the first split portion of the key with the encryption key/decryption key.

**Regarding claim 14**, Merrick discloses wherein said step of combining said first key portion and said second key portion utilizes an "exclusive or" logic operation performed by said hardware product (claim 7; a combiner combining first and second key portions to generate a full length key). It is obvious that the combiner used in Merrick is an "exclusive or" logic. But the examiner provides reference Rasmussen that discloses xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK) using an exclusive or operator see, fig. 4 element 144 and col. 8 lines 40-48.Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of excusive or within the combination system to combine the first encryption key and first key portion because operator exclusive or necessary for combining. One would have been motivated to do so to combine the first split portion of the key with the encryption key/decryption key.

**Regarding claim 28**, Nakamura discloses the method wherein said first key portion is generated independent of information generated in or by said hardware product (Nakamura, col. 18 lines 50-61, col. 19 lines 37-59, fig. 12 & 13, claim 11, col. 6 lines 38-39, and col. 3 lines 20-22). The rational for combining are the same as claim 11 above.

**Regarding claim 29**, Nakamura discloses the method wherein said second key portion is generated independent of said hardware product and any information specific to, identifying, or generated in or by said hardware product (Nakamura col. 18 lines 50-61, col. 19 lines 37-59, fig. 12 & 13, claim 11, col. 6 lines 38-39, and col. 3 lines 20-22). The rational for combining are the same as claim 11 above.

**Regarding claim 30**, Nakamura discloses wherein said first encryption key is generated independent of said hardware product and any information specific to, identifying, or generated in or by said hardware product (Nakamura col. 2 lines 52-59 and col. 14 lines 13- 19). The rational for combining are the same as claim 11 above.

**11. Claims 15-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merrick in view of Nakamura and Chan and further in view of Kitajima.**

**Regarding claim 15**, Merrick, Nakamura and Chan teach all the subject matter as described above. In addition the combination discloses the method further enabling security of said first encryption key and providing a second encryption key for encrypting a different version of the initial software product, further comprising: generating the second encryption key (Merrick fig. 1 element 40;full key~full-length key of N/N bits); encrypting the different version of the initial software product with said second encryption key to provide an encrypted different version of the initial software product (Merrick col. 2 lines 26-27 and claim 1; encrypting data using key of length N); combining said first encryptiOn key and said second encryption key to provide a third key portion (Merrick col. 5 lines 33-52); installing said third key portion in said tamper proof memory means (Chan col. 5 lines 44-45); installing said encrypted different version of the initial software product in said further memory means in the hardware product (Merrick col. 5 lines 33); combining said third key portion and said second key portion to generate a fourth key portion in the hardware product (Merrick col. 5 lines 33-52); combining said first key portion and said fourth key portion to provide said second encryption key in the hardware product (Merrick col. 5 lines 33-52); and using said second encryption key in the hardware product to decrypt the encrypted different version of the initial software product (Merrick col. 5 lines 33-52 and claims 1, 6-7). The rational for combining are the same as claim 11 above. Merrick, Nakamura et al. and Chan fail to teach an update of the keys. However Kitajima discloses dividing encrypting key into a first half portion and a second half portion and periodically updating/changing keys and encryption algorithm to securely protect cryptograms against unauthorized people (col. 11 lines 1-10). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of updating keys within the combination system because it would allow a secure data/ message/ information transmission (col. 11 lines 1-10). One would have been motivated to update the encryption key and the key portions to enhance security by making the keys unpredictable.

**Regarding claim 16**, references discloses the method wherein said step of generating a second encryption key utilizes a ransom number generator to generate said first encryption key (Merrick col. 5 lines 5-16, Nakamura col. 13 lines 51-57, Chan col. 5 lines 39-64).

**Regarding claim 17**, Merrick teaches the method wherein said step of combining said first encryption key and said second encryption key to generate a third key portion utilizes an "exclusive or" logic operation (claim 7; a combiner combining first and second key portions to generate a full length key). It is obvious that the combiner used in Merrick is an "exclusive or" logic. But the examiner provides reference Rasmussen et al. Patent Number: 5,301,247 that discloses xoring first portion of key (DEK 1) with second portion (DEK2) of key to form encryption key (DEK) using an exclusive or operator see, fig. 4 element 144 and col. 8 lines 40- 48.Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of excusive or within the combination system to combine said first encryption key and said second encryption key and generate said third key portion because operator exclusive or necessary for combining. One would have been motivated to do so to combine first encryption key and said second encryption key.

**Regarding claim 18**, Merrick teaches wherein said step ofcombining said first key portion and the fourth key portion to provide said second encryption key utilizes an "exclusive or" logic operation (claim 7; a combiner combining first and second key portions to generate a full length key). It is obvious that the combiner used in Merrick is an "exclusive or" logic. But the examiner provides reference Rasmussen et al. Patent Number: 5,301,247 that discloses xoring first portion of key (DEK 1) with second portion (DEK2) of key to form encryption key (DEK) using an exclusive or operator see, fig. 4 element 144 and col. 8 lines 40-48.The rational for combining are the same as claim 17 above.

**12. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Merrick in view of Nakamura and Chan and further in view of Vincent.**

**Regarding claim 19**, the combination discloses all the subject matter as described. The combination fail to disclose wherein said initial version of software product and said different version of said initial version of said software product are non-sequential versions. However Vincent discloses updating required versions out of multiple different versions of software products in non-sequential order (fig. 9 and par. 0071 ; updating component B from version 4 to version 6 and updating full component of D and E to version 1 and 2 respectively). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Vincent within the combination system because it would save time (par. 0015). One would have been motivated to update non-sequential version of software because it would allow a minimal time to download specific software components in contrast to conventional methods of updating software (par. 0015).

**13. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Merrick in view of Nakamura and Chan and further in view of Mizikovsky.**

**Regarding claim 20**, the combination discloses all the subject matter as described. The combination fail to teach wherein the second encryption key is non-sequential with said first encryption key. However Mizikovsky teaches an update key which is non-sequential with said first encryption key (col. 8 lines 21-43 and fig. 4; update key being different from new key...generated in using RAND numbers). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Mizikovsky within the combination system because it would enhance security. One would have been motivated to incorporate the teachings of updating keys in non-sequential order to prevent unauthorized device from learning encryption keys and perform unauthorized decryption of content.

### *Conclusion*

14. **Examiner's Note:** Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

17. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

18. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

9/29/07